

FILED

AUG 10 2022

2021R00546

AT 8:30 *SWS*
 WILLIAM T. WALSH *PM*
 CLERK *JB*

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA

v.

MANSOUR AHMADI,
a/k/a "Mansur Ahmadi,"AHMAD KHATIBI AGHDA,
a/k/a "Ahmad Khatibi," andAMIR HOSSEIN NICKAEIN RAVARI,
a/k/a "Amir Hossein Nikaeen,"
a/k/a "Amir Hossein Nickaein,"
a/k/a "Amir Nikayin"

: Hon. Brian R. Martinotti

: Criminal No. 22-541

: 18 U.S.C. § 2

: 18 U.S.C. § 371

: 18 U.S.C. § 1030(a)(5)(A)

: 18 U.S.C. § 1030(a)(7)(C)

:

:

:

:

:

:

I N D I C T M E N T

The Grand Jury in and for the District of New Jersey, sitting at Newark charges:

COUNT ONE
**(Conspiracy to Commit Fraud and
Related Activity in Connection with Computers)**

Overview

1. From at least in or around October 2020 through the date of this Indictment, defendants MANSOUR AHMADI, a/k/a "Mansur Ahmadi," ("AHMADI"), AHMAD KHATIBI AGHDA, a/k/a "Ahmad Khatibi," ("KHATIBI"), and AMIR HOSSEIN NICKAEIN RAVARI, a/k/a "Amir Hossein Nikaeen," a/k/a "Amir Hossein Nickaein," a/k/a "Amir Nikayin" ("NICKAEIN"), and known and unknown co conspirators engaged in a scheme to gain unauthorized access to the computer systems of hundreds of victims in the United States, the United

Kingdom, Israel, Iran, Russia, and elsewhere, causing damage and loss to those victims. The defendants' persistent hacking campaign exploited known vulnerabilities in commonly used network devices and software applications to access and exfiltrate data and information from victims' computer systems. As part of this scheme, KHATIBI, NICKAEIN, and others profited by conducting encryption attacks against victims' computer systems and then denying victims access to their systems and data unless they made a ransom payment.

2. Over the course of their scheme, AHMADI, KHATIBI, NICKAEIN, and others victimized a broad range of organizations, including small businesses, government agencies, non-profit programs, and educational and religious institutions. Their victims also included multiple critical infrastructure sectors, including healthcare centers, transportation services, and utility providers.

3. At all times relevant to this Indictment:

The Defendants

a. AHMADI was a citizen and resident of Iran who owned and controlled a technology company in Iran.

b. KHATIBI was a citizen and resident of Iran who owned a separate technology company in Iran.

c. NICKAEIN was a citizen and resident of Iran who worked for KHATIBI's technology company.

The Victims

d. "The Township" was a municipality in Union County, New Jersey.

- e. "Accounting Firm 1" was an accounting firm based in Morris County, New Jersey.
- f. "Accounting Firm 2" was an accounting firm based in Illinois.
- g. "Power Company 1" was a regional electric utility company based in Mississippi.
- h. "Power Company 2" was a regional electric utility company based in Indiana.
- i. "The Housing Authority" was a public housing corporation in the State of Washington.
- j. "The Domestic Violence Shelter" was a shelter for victims of domestic violence in Pennsylvania.
- k. "The County" was a County government in Wyoming.
- l. "The Construction Company" was a construction company located in the State of Washington that was engaged in work on critical infrastructure projects.
- m. "The Bar Association" was the official state bar association of a state in the United States.

Relevant Terms

- n. "Bitcoin" was a type of cryptocurrency circulated over the internet as a form of value. Bitcoin were not issued by any government, bank, or company, but rather were generated and controlled through computer software operating via a decentralized peer-to-peer network. Bitcoin fluctuates in value. On or about October 1, 2020, one bitcoin was worth approximately

\$11,000. On or about June 16, 2022, one bitcoin was worth approximately \$21,000.

o. A Bitcoin “wallet” was a digital wallet that stored Bitcoin and enabled transactions in Bitcoin. A Bitcoin wallet was designed both to hold the digital currency and ensure that only the owner of the wallet could access that currency.

p. “Fast Reverse Proxy” or “FRP” was a publicly available cyber tool that could be used for both legitimate and illegitimate purposes. FRP could be used to maintain unauthorized “back door” connections to victim networks.

q. “BitLocker” was a commercially available software and security feature used to secure data. BitLocker was frequently included in common operating systems as a security feature for data encryption. Individuals who access a victim’s network without authorization and to launch cyber attacks could use BitLocker to encrypt victims’ data and prevent victims from accessing their data.

The Conspiracy

4. From at least in or around October 2020 through the date of this Indictment, in Union and Morris Counties, in the District of New Jersey, and elsewhere, the defendants,

MANSOUR AHMADI,
a/k/a “Mansur Ahmadi,”

AHMAD KHATIBI AGHDA,
a/k/a “Ahmad Khatibi,” and

AMIR HOSSEIN NICKAEIN RAVARI,
a/k/a “Amir Hossein Nikaeen,”

a/k/a "Amir Hossein Nickaein,"
a/k/a "Amir Nikayin,"

did knowingly and intentionally conspire and agree to commit offenses against the United States, that is:

a. to knowingly cause the transmission of a program, information, code, or command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to persons during a one-year period from Defendants' course of conduct affecting protected computers aggregating at least \$5,000 in value, and cause damage affecting 10 or more protected computers during a one-year period, contrary to Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B); and

b. to knowingly and with intent to extort from any person any money or other thing of value, transmit in interstate and foreign commerce any communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, contrary to Title 18, United States Code, Sections 1030(a)(7)(C) and (c)(3)(A).

Goal of the Conspiracy

5. The goal of the conspiracy was for the Defendants, acting from inside Iran, to obtain and maintain unauthorized access to victims' computers and to accomplish the following objectives, among others, depending on the particular intrusion: (i) control victims' computer systems; (ii) steal victims' data; (iii) cause damage to victims' computers, including by encrypting victim data; and

(iv) demand ransom payments from victims in exchange for maintaining the confidentiality of victims' stolen data or decrypting their data.

Manner and Means of the Conspiracy

6. It was part of the conspiracy that:

a. AHMADI, KHATIBI, NICKAEIN, and their co-conspirators exploited vulnerabilities in victims' computer systems to gain unauthorized access and control over these systems.

b. AHMADI, KHATIBI, NICKAEIN, and their co-conspirators used FRP to maintain unauthorized access to victims' computer systems.

c. AHMADI, KHATIBI, NICKAEIN, and their co-conspirators created and registered "look-alike" web domains using a naming format that was designed to resemble the web domains of legitimate, well-known, technology companies in order to deceive victims and disguise the illegal activities.

d. AHMADI, KHATIBI, NICKAEIN, and their co-conspirators stole and caused others to steal data from victims' computer systems.

e. AHMADI, KHATIBI, NICKAEIN, and their co-conspirators conducted and caused others to conduct encryption attacks against victims by activating BitLocker on victim networks, thereby denying victims access to their systems and data unless their victims made a ransom payment in exchange for the BitLocker decryption keys.

f. AHMADI, KHATIBI, NICKAEIN, and their co-conspirators collected payments in Bitcoin and other cryptocurrencies from certain victims that paid the ransom to decrypt their data.

Overt Acts

7. In furtherance of the conspiracy, and in order to effect its objects, defendants AHMADI, KHATIBI, NICKAEIN, and their co-conspirators committed and caused to be committed the following overt acts in the District of New Jersey, and elsewhere:

The Township Compromise

a. On or about January 6, 2021, AHMADI registered a website address ("Domain 1") with a U.S. company. Domain 1 used a name that resembled a major U.S. technology company, but in fact had no relationship to that company.

b. In or around February 2021, a member of the conspiracy gained unauthorized access to the computer system of the Township, thereby gaining control and access to the Township's network and data.

c. In or around February 2021, using this unauthorized access, a member of the conspiracy installed FRP on the Township's network to establish an unauthorized connection from the Township's network to Domain 1.

Compromise, Malicious Encryption, and Extortion of Accounting Firm 2

d. Prior to on or about April 19, 2021, NICKAEIN gained unauthorized access to the computer system of Accounting Firm 2, stole data, and launched an encryption attack using BitLocker, thereby denying Accounting Firm 2 access to certain of its systems and data.

e. On or about April 19, 2021, NICKAEIN sent a ransom demand communication to the printers at Accounting Firm 2. The note demanded

payment in exchange for decrypting the data and also threatened to publicize the stolen data if payment was not made. The note directed Accounting Firm 2 to contact an email account controlled by NICKAEIN. The ransom demand read in part as follows:

Hi!
IF YOU ARE READING THIS, IT MEANS YOUR DATA IS
ENCRYPTED AND YOUR PRIVATE SENSITIVE
INFORMATION IS STOLEN!
READ CAREFULLY THE WHOLE INSTRUCTIONS TO AVOID ANY
PROBLEMS
YOU HAVE TO CONTACT US IMMEDIATELY TO RESOLVE THIS
ISSUE AND MAKE A DEAL!

...

We will sell your data if you decide not to pay or try to recover them.

Compromises of Power Company 1 and Power Company 2

f. On or about October 6, 2021, and again on or about October 14, 2021, KHATIBI visited Power Company 1's website.

g. Prior to on or about October 14, 2021, KHATIBI gained unauthorized access to Power Company 1's computer system and launched an encryption attack by activating BitLocker, thereby denying Power Company 1 access to some of its systems and data.

h. On or about October 14, 2021, KHATIBI printed a ransom demand to Power Company 1's printers. The ransom demand directed Power Company 1 to contact an email account or messaging platform account, both of which were controlled by KHATIBI, and read in part as follows:

- A. You read this text because your network is accessible to us.
- B. We can block re-hacking. you are constantly at risk.
- C. If you want to secure your network against any hacking and get your encrypted codes, Contact us.
..
- i. On or about October 25, 2021, KHATIBI gained unauthorized access to Power Company 2's computer system and attempted to launch an encryption attack using BitLocker.

*Compromise, Malicious Encryption, and Extortion of
The Domestic Violence Shelter*

j. On or about December 12, 2021, a member of the conspiracy gained unauthorized access to the Domestic Violence Shelter's computer system and launched an encryption attack by activating BitLocker, thereby denying the Domestic Violence Shelter access to some of its systems and data.

k. On or about December 12, 2021, a member of the conspiracy printed a note to the printers at the Domestic Violence Shelter stating, "Hi. Do not take any action for recovery. Your files may be corrupted and not recoverable. Just contact us." The note directed the Domestic Violence Shelter to contact an email account or messaging platform account that was controlled by KHATIBI.

l. On or about December 21, 2021, KHATIBI sent an email to a representative of the Domestic Violence Shelter asking for payment of one Bitcoin.

m. After agreeing to a price of \$13,000, KHATIBI provided his Bitcoin wallet address to the Domestic Violence Shelter representative for payment.

n. After receiving payment from the Domestic Violence Shelter, KHATIBI provided decryption keys to enable the Domestic Violence Shelter to restore access to its systems and data.

Compromise, Malicious Encryption, and Extortion of the Housing Authority

o. Prior to on or about January 8, 2022, a member of the conspiracy gained unauthorized access to the Housing Authority's computer system, stole data, and launched an encryption attack by activating BitLocker, thereby denying the Housing Authority access to some of its systems and data.

p. On or about January 8, 2022, a member of the conspiracy also placed a note on a Housing Authority computer directing them to contact an email account or messaging platform account, both of which were controlled by KHATIBI.

q. Between on or about January 28, 2022, and on or about February 3, 2022, KHATIBI communicated with representatives of the Housing Authority via email. In one email on or about February 1, 2022, KHATIBI threatened to sell the data stolen from the Housing Authority. KHATIBI stated in part:

I want this to end, and if you do not want to pay, let me know so that I can make money by selling data.

Before you, the Iranian [Company] did not want to pay \$500,000, and I received more through the sale of their data.

Compromise, Malicious Encryption, and Extortion of the Construction Company

r. On or about December 5, 2021, NICKAEIN leased and registered a computer server (“Server 1”) for use in cyber attacks by members of the conspiracy.

s. On a date no later than on or about February 16, 2022, a member of the conspiracy gained unauthorized access to the computer systems of the Construction Company.

t. Between on or about February 16, 2022, and on or about February 25, 2022, using the FRP tool, a member of the conspiracy caused servers on the Construction Company’s network to connect to Server 1 and stole data.

u. On or about February 22, 2022, KHATIBI activated BitLocker to encrypt the Construction Company’s data and deny it access to some of its systems.

v. On or about February 22, 2022, KHATIBI sent a note to the Construction Company’s printer with a contact address for a messaging application controlled by KHATIBI.

w. On or about February 22, 2022, via messaging application, KHATIBI informed a representative of the Construction Company, “I locked more than 90 systems on your network” and asked, “Are you ready to pay?” KHATIBI demanded \$200,000 and provided his Bitcoin wallet for payment, namely, the same wallet he provided to the Domestic Violence Shelter.

Compromise, Malicious Encryption, and Extortion of Accounting Firm 1

x. On a date no later than on or about February 27, 2022, a member of the conspiracy gained unauthorized access to Accounting Firm 1's computer system.

y. Between on or about February 27, 2022, and on or about March 1, 2022, using the FRP tool, a member of the conspiracy caused a server on Accounting Firm 1's network to connect to Server 1 and stole data.

z. On a date no later than on or about March 2, 2022, a member of the conspiracy launched an encryption attack against Accounting Firm 1 using BitLocker, thereby denying Accounting Firm 1 access to some of its systems.

aa. On or about March 8, 2022, KHATIBI emailed a representative of Accounting Firm 1, asking, "Are you ready to pay?"

bb. On or about March 9, 2022, KHATIBI emailed again, stating that he had "locked more than 20 systems" and asking for "\$50,000."

cc. On or about March 16, 2022, KHATIBI emailed a representative of Accounting Firm 1 and stated, "If you don't want to pay, I can sell your data on the black market. This choice is yours."

Compromise of the County

dd. On a date no later than on or about March 8, 2022, a member of the conspiracy gained unauthorized access to the computer systems of the County.

ee. Between on or about March 8, 2022, and on or about May 2, 2022, using the FRP tool, a member of the conspiracy caused servers on the County's network to connect to Server 1.

ff. On or about March 28, 2022, NICKAEIN accessed the County's website.

gg. Prior to on or about April 3, 2022, KHATIBI accessed the County's computer system without authorization and stole data.

Compromise, Malicious Encryption, and Extortion of the Bar Association

hh. Prior to on or about April 28, 2022, a member of the conspiracy gained unauthorized access to the computer systems of the Bar Association.

ii. On or about April 28, 2022, using the FRP tool, a member of the conspiracy caused servers on the Bar Association's computer network to connect to Server 1.

jj. On or about April 28, 2022, a member of the conspiracy launched an encryption attack against the Bar Association by activating BitLocker, thereby denying the Bar Association access to its systems and data. The ransom note directed the Bar Association to contact an email address and messaging application account, both of which were controlled by KHATIBI—the same accounts KHATIBI had used in his ransom negotiations with previous victims.

Documenting Illegal Acts

kk. Between on or about April 26, 2021, and on or about February 24, 2022, AHMADI emailed another individual timesheets reflecting the hours worked by NICKAEIN, KHATIBI, and others, including, in certain instances, tasks performed in connection with cyber attacks and in furtherance of the conspiracy.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO
(Intentional Damage to a Protected Computer)

1. The allegations in paragraphs 1, 2, 3, 5, 6, and 7 of Count One of this Indictment are re-alleged here.
2. In or around February 2021, in Union County, in the District of New Jersey, and elsewhere, the defendant,

MANSOUR AHMADI,
a/k/a "Mansur Ahmadi,"

knowingly caused the transmission of a program, information, code, and command and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, that is, the computer network at the Township used in and affecting interstate and foreign commerce and communication, and the offense caused loss to persons during a one-year period from Defendant's course of conduct affecting protected computers aggregating at least \$5,000 in value, and caused damage affecting 10 or more protected computers during a one-year period.

In violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B), and Section 2.

COUNT THREE
(Intentional Damage to a Protected Computer)

1. The allegations in paragraphs 1, 2, 3, 5, 6, and 7 of Count One of this Indictment are re-alleged here.

2. On or about February 27, 2022 through on or about March 2, 2022, in Morris County, in the District of New Jersey, and elsewhere, the defendants,

MANSOUR AHMADI,
a/k/a "Mansur Ahmadi,"

AHMAD KHATIBI AGHDA,
a/k/a "Ahmad Khatibi," and

AMIR HOSSEIN NICKAEIN RAVARI,
a/k/a "Amir Hossein Nikaein,"
a/k/a "Amir Hossein Nickaein,"
a/k/a "Amir Nikayin,"

knowingly caused the transmission of a program, information, code, and command and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, that is, the computer network at Accounting Firm 1 used in and affecting interstate and foreign commerce and communication, and the offense caused loss to persons during a one-year period from Defendants' course of conduct affecting protected computers aggregating at least \$5,000 in value, and caused damage affecting 10 or more protected computers during a one-year period.

In violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B), and Section 2.

COUNT 4

(Transmitting a Demand in Relation to Damaging a Protected Computer)

1. The allegations in paragraphs 1, 2, 3, 5, 6, and 7 of Count One of this Indictment are re-alleged here.
2. On or about March 9, 2022, in the District of New Jersey, and elsewhere, the defendants,

MANSOUR AHMADI,
a/k/a "Mansur Ahmadi,"

AHMAD KHATIBI AGHDA,
a/k/a "Ahmad Khatibi," and

AMIR HOSSEIN NICKAEIN RAVARI,
a/k/a "Amir Hossein Nikaeen,"
a/k/a "Amir Hossein Nickaein,"
a/k/a "Amir Nikayin,"

with intent to extort from Accounting Firm 1 money and other things of value, transmitted in interstate and foreign commerce a communication containing a demand and request for money and other things of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

In violation of Title 18, United States Code, Sections 1030(a)(7)(C) and (c)(3)(A), and Section 2.

FORFEITURE ALLEGATIONS

1. Upon conviction of any of the offenses charged in this Indictment, the defendants charged in each respective count, shall forfeit to the United States:

- a. pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offenses charged in this Indictment; and
- b. pursuant to 18 U.S.C. § 1030(i), all right, title, and interest of the defendant in any personal property that was used or intended to be used to commit or to facilitate the commission of the offenses charged in this Indictment.

SUBSTITUTE ASSETS PROVISION

2. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States shall be entitled, pursuant to 21 U.S.C. § 853(p) (as incorporated by 28 U.S.C. § 2461(c), 18 U.S.C. § 1030(i), and 18 U.S.C. § 982(b)), to forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

A TRUE BILL

[REDACTED] _____
FOREPERSON



PHILIP R. SELLINGER
United States Attorney

CASE NUMBER: 22-541 (BRM)

**United States District Court
District of New Jersey**

UNITED STATES OF AMERICA

v.

**MANSOUR AHMADI,
a/k/a "Mansur Ahmadi,"**

**AHMAD KHATIBI AGHDA,
a/k/a "Ahmad Khatibi," and**

**AMIR HOSSEIN NICKAEIN RAVARI,
a/k/a "Amir Hossein Nikaeen,"
a/k/a "Amir Hossein Nickaein,"
a/k/a "Amir Nikayin"**

INDICTMENT FOR

18 U.S.C. §§ 2, 371, 1030(a)(5)(A), 1030(a)(7)(C)

A



Forepers n

**PHILIP R. SELLINGER
UNITED STATES ATTORNEY
FOR THE DISTRICT OF NEW JERSEY**

**DAVID MALAGOLD
MATTHEW NIKIC
ASSISTANT U.S. ATTORNEYS, DISTRICT OF NEW JERSEY**

**ANDREW BEATY
TRIAL ATTORNEY, U.S. DEPARTMENT OF JUSTICE
WASHINGTON, D.C.**
